

## PATENT COOPERATION TREATY

## PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY  
(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

REC'D 31 MAR 2006

WIPO

PCT

Applicant's or agent's file reference 030457WO	FOR FURTHER ACTION		See Form PCT/IPEA/416																
International application No. PCT/US04/36284	International filing date ( <i>day/month/year</i> ) 28 October 2004 (28.10.2004)	Priority date ( <i>day/month/year</i> ) 29 October 2003 (29.10.2003)																	
International Patent Classification (IPC) or national classification and IPC IPC: H04L 9/00 USPC: 713/176,168;705/76																			
Applicant QUALCOMM INCORPORATED																			
<p>1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.</p> <p>2. This REPORT consists of a total of <u>5</u> sheets, including this cover sheet.</p> <p>3. This report is also accompanied by ANNEXES, comprising:</p> <p>a. <input type="checkbox"/> (<i>sent to the applicant and to the International Bureau</i>) a total of <u>    </u> sheets, as follows:</p> <p style="margin-left: 40px;"><input type="checkbox"/> sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).</p> <p style="margin-left: 40px;"><input type="checkbox"/> sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.</p> <p>b. <input type="checkbox"/> (<i>sent to the International Bureau only</i>) a total of (indicate type and number of electronic carrier(s)) <u>    </u>, containing a sequence listing and/or tables related thereto, in electronic form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).</p> <p>4. This report contains indications relating to the following items:</p> <table border="0" style="width: 100%;"> <tr> <td><input checked="" type="checkbox"/> Box No. I</td> <td>Basis of the report</td> </tr> <tr> <td><input type="checkbox"/> Box No. II</td> <td>Priority</td> </tr> <tr> <td><input type="checkbox"/> Box No. III</td> <td>Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</td> </tr> <tr> <td><input type="checkbox"/> Box No. IV</td> <td>Lack of unity of invention</td> </tr> <tr> <td><input checked="" type="checkbox"/> Box No. V</td> <td>Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</td> </tr> <tr> <td><input type="checkbox"/> Box No. VI</td> <td>Certain documents cited</td> </tr> <tr> <td><input type="checkbox"/> Box No. VII</td> <td>Certain defects in the international application</td> </tr> <tr> <td><input type="checkbox"/> Box No. VIII</td> <td>Certain observations on the international application</td> </tr> </table>				<input checked="" type="checkbox"/> Box No. I	Basis of the report	<input type="checkbox"/> Box No. II	Priority	<input type="checkbox"/> Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability	<input type="checkbox"/> Box No. IV	Lack of unity of invention	<input checked="" type="checkbox"/> Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement	<input type="checkbox"/> Box No. VI	Certain documents cited	<input type="checkbox"/> Box No. VII	Certain defects in the international application	<input type="checkbox"/> Box No. VIII	Certain observations on the international application
<input checked="" type="checkbox"/> Box No. I	Basis of the report																		
<input type="checkbox"/> Box No. II	Priority																		
<input type="checkbox"/> Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability																		
<input type="checkbox"/> Box No. IV	Lack of unity of invention																		
<input checked="" type="checkbox"/> Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement																		
<input type="checkbox"/> Box No. VI	Certain documents cited																		
<input type="checkbox"/> Box No. VII	Certain defects in the international application																		
<input type="checkbox"/> Box No. VIII	Certain observations on the international application																		
Date of submission of the demand 31 May 2005 (31.05.2005)		Date of completion of this report 16 March 2006 (16.03.2006)																	
Name and mailing address of the IPEA/US Mail Stop PCT, Attn: IPEA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201		Authorized officer <i>for [Signature]</i> Joseph Pan Telephone No. 571-272-5987																	

Form PCT/IPEA/409 (cover sheet)(April 2005)

## INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.

PCT/US04/36284

## Box No. I Basis of the report

1. With regard to the language, this report is based on:

- ☐ the international application in the language in which it was filed.
- ☐ a translation of the international application into \_\_\_\_\_, which is the language of a translation furnished for the purposes of:
- ☐ international search (under Rules 12.3 and 23.1(b))
- ☐ publication of the international application (under Rule 12.4(a))
- ☐ international preliminary examination (under Rules 55.2(a) and/or 55.3(a))

2. With regard to the elements of the international application, this report is based on (replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report):

- ☒ the international application as originally filed/furnished
- ☒ the description:  
pages 1-5 \_\_\_\_\_ as originally filed/furnished  
pages\* NONE \_\_\_\_\_ received by this Authority on \_\_\_\_\_  
pages\* NONE \_\_\_\_\_ received by this Authority on \_\_\_\_\_
- ☒ the claims:  
pages 5-8 \_\_\_\_\_ as originally filed/furnished  
pages\* NONE \_\_\_\_\_ as amended (together with any statement) under Article 19  
pages\* NONE \_\_\_\_\_ received by this Authority on \_\_\_\_\_  
pages\* NONE \_\_\_\_\_ received by this Authority on \_\_\_\_\_
- ☒ the drawings:  
pages 1-9 \_\_\_\_\_ as originally filed/furnished  
pages\* NONE \_\_\_\_\_ received by this Authority on \_\_\_\_\_  
pages\* NONE \_\_\_\_\_ received by this Authority on \_\_\_\_\_
- ☐ a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing.

- 3.
- ☐
- The amendments have resulted in the cancellation of:

- ☐ the description, pages \_\_\_\_\_
- ☐ the claims, Nos. \_\_\_\_\_
- ☐ the drawings, sheets/figs \_\_\_\_\_
- ☐ the sequence listing (specify): \_\_\_\_\_
- ☐ any table(s) related to the sequence listing (specify): \_\_\_\_\_

- 4.
- ☐
- This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

- ☐ the description, pages \_\_\_\_\_
- ☐ the claims, Nos. \_\_\_\_\_
- ☐ the drawings, sheets/figs \_\_\_\_\_
- ☐ the sequence listing (specify): \_\_\_\_\_
- ☐ any table(s) related to the sequence listing (specify): \_\_\_\_\_

\* If item 4 applies, some or all of those sheets may be marked "superseded."  
Form PCT/IPEA/409 (Box No. I) (April 2005)

## INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.  
PCT/US04/36284**Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement****1. Statement**

Novelty (N)

Claims 1-45 YESClaims NONE NO

Inventive Step (IS)

Claims NONE YESClaims 1-45 NO

Industrial Applicability (IA)

Claims 1-45 YESClaims NONE NO**2. Citations and Explanations (Rule 70.7)**

Please See Continuation Sheet

## Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

Continuation of:

## V. 2. Citations and Explanations:

Claims 1-45 lack inventive step under PCT article 33(3) as being obvious over Drews (U.S. Patent No. 6,477,645) in view of Bari et al. (U.S. Pub. No. 2002/0023059).

Drews discloses referring to FIG. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking a public key is shown. System 100 includes remote platform 105, user platform 110, including transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation value 135, information transformation value 140, or credential subset transformation value 145, from authorizing entity 150 for input into comparison system 120 of user platform 110. Remote platform 105 is capable of receiving information 155 and credential 160, which includes credential subset 165 from authorizing entity 150.

Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, such as a cell phone, or a television or radio transmitter or transceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.

The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information 155 is a boot image, but those skilled in the art will recognize that the present invention is equally applicable to the transmission of information such as application software or data.

Credential 160, in one embodiment, contains authority information, such as a digital signature or digital signature in combination with other information, such as a digital certificate that normally accompanies transmitted information. The authority information, without a public key that designates the authorized source of the

## Supplemental Box

credential's digital signature installed on user platform 110, is insufficient to check the authority of the credential. However, a credential which includes a digital signature that covers the rest of the credential can be used to check the integrity of the credential.

User platform 110 is provided for the purpose of receiving transmitted information such as information 155, credential 160, or information 155 and credential 160 from remote platform 105. User platform 110 is the target device for software, commands, or data staged on remote platform 105, and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, such as a pager, a cell phone, or a television or radio receiver or transceiver. Like remote platform 105, user platform 110 is not limited to any particular type of device, and those skilled in the art will recognize that any device capable of receiving information from remote platform 105 can be used in the present invention. (see column 2, lines 9-55 of Drows).

Transformation value generator 115 is provided to convert a variable length amount of digital data into a more concise form. In one embodiment of the invention, generator 115 is a hash function. A hash function accepts any length input and generates a fixed length output. Hash functions are known in the art and those skilled in the art will recognize that a hash function suitable for use in embodiments of the present invention is one that is relatively easy to compute, one-way, and collision-free. (see column 3, lines 15-23 of Drows).

In one embodiment, authorizing entity 150 supplies information transformation value 140, computed from information 155, to user 130. The transformation value is computed such that all parts of the information contribute to the transformation value in a way that is one-way and collision-free. In one embodiment, user platform 110 receives information transformation value 140 from user 130. Comparison system 120 compares the received information transformation value 140 with the output of transformation value generator 115, which generates a transformation value of information 155 supplied by remote platform 105. A match authenticates information 155 by ensuring the integrity and the authority of information 155. (see column 4, lines 24-37 of Drows).

Drows discloses the claimed subject matter. However, Drows does not specifically mention using the master credential in generating the application credential. On the other hand, Bari et al. disclose a system for registering, storing and managing personal data for use over a network, wherein the master credential is utilized (see paragraph [0046], lines 10-19 of Bari et al.). It would have been obvious to a person of ordinary skill in the art at the time the invention to utilize the master credential in generating the application credential. The ordinary skilled person would have been motivated to have applied the teaching of Bari et al. into method of Drows to utilize the master credential, because once a user is registered, the inventive system recognizes and authenticates the Master Authentication Credential, which then unlocks the personalized vault containing Authentication Master Credential for third party Web Sites and the User Profile (see paragraph [0036], lines 19-23 of Bari et al.).

Claims 1-45 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.